TITLE OF THE INVENTION
暗号化コンテンツ記録媒体、再生装置および再生方法

BACKGROUND OF THE INVENTION
(1)FIELD OF THE INVENTION
本発明は、著作権保護されているコンテンツの再生装置、再生方法、およびそれらに用いられるデータが格納された記録媒体に関する。

(2)PRIOR ART
ＤＶＤ（Ｄｉｇｉｔａｌ　Ｖｅｒｓａｔｉｌｅ　Ｄｉｓｃ）では、コンテンツの不正なコピーを防止するために、ＣＳＳ（Ｃｏｎｔｅｎｔｓ　Ｓｃｒａｍｂｌｉｎｇ　Ｓｙｓｔｅｍ）が導入されている。ＣＳＳでは、ＤＶＤメディアに対して固有の情報を記録し、この情報及び再生機器が保持する情報からタイトル鍵を生成する。こうして生成されたタイトル鍵を用いて、ＤＶＤメディアに記録された暗号化コンテンツを復号して再生する（例えば特開２００３－３７５８９号公報参照）。
一方、近年デジタル著作権管理（ＤＲＭ：Ｄｉｇｉｔａｌ　Ｒｉｇｈｔｓ　Ｍａｎａｇｅｍｅｎｔ）システムを用いたコンテンツ配信システムも一般的になりつつある。ＤＲＭでは暗号化コンテンツとは別にライセンスが配信される。ライセンスにはライセンス鍵と利用条件が記録されており、この利用条件に従って、コンテンツをライセンス鍵で復号して再生する。
ＤＲＭでは、コンテンツ及びライセンスはネットワークを介して配信される。さらに近年はコンテンツをサーバ型放送と呼ばれる蓄積型の放送システムで配信する試みも成されようとしている。
さて、近年これまでのＤＶＤに代わるメディアとしてＢＤ（Ｂｌｕ－ｒａｙ　Ｄｉｓｃ）が提案されている。ＢＤはＤＶＤの５倍程度の容量を持ち、これまでのＳＤ画質の映像だけではなくＨＤ画質の映像を記録することも可能となる。
ＢＤでは、従来のＤＶＤにおけるＣＳＳと同様に、メディアに固有の情報を記録して、この情報及び再生機器が保持する情報からメディア鍵を生成する仕組みを備える。さらに、こうして得られたメディア鍵を用いてコンテンツを暗号化し、暗号化されたコンテンツがメディアには記録される。このような方法によって、ＤＶＤと同様にコンテンツの不正なコピーが防止される。
さらに、ＢＤではＤＲＭの適用も検討されている。パッケージメディアにＤＲＭを適用する場合には、ライセンス鍵で暗号化されたコンテンツをメディアに格納し、ライセンスは別途ネットワークを介して配信することになる。再生時には、メディアに記録された暗号化コンテンツをライセンス鍵で復号して再生する。
しかしながら、このようなＤＲＭ適用においては、メディア上で従来型のコピー防止がなされたコンテンツとＤＲＭが適用されたコンテンツが混在する場合に問題が発生する。このようなケースでは、再生プレイヤーは当該コンテンツが従来型のコピー防止がなされたコンテンツなのか、ＤＲＭが適用されたコンテンツなのかがわからないという課題があった。もしも、ＤＲＭが適用されたコンテンツをメディア鍵で復号すれば、コンテンツは復号することができない。逆に従来型のコピー防止がなされたコンテンツに大して対応するライセンスを検索したとしても、対応するライセンスは存在しないために再生することができない。

SUMMARY OF THE INVENTION
それゆえ、本発明の目的は、従来型のコピー防止がなされたコンテンツとＤＲＭが適用されたコンテンツが混在するメディアにおいて、双方のコンテンツを適切に再生するために適したデータ構造を提供し、さらに当該データ構造を有するデータを格納した記録媒体、ならびにそれを再生するための再生装置および再生方法を提供することである。

上記課題を解決するために、本発明では、暗号化コンテンツとメディアに固有なメディ

ア鍵が記録された媒体を再生する端末であって、少なくとも前記暗号化コンテンツの復号鍵を含むライセンスを取得するライセンス取得手段と、前記ライセンスからコンテンツ鍵を取得するコンテンツ鍵取得手段と、前記暗号化コンテンツの復号に前記メディア鍵とコンテンツ鍵の何れを用いるかを判定する鍵選択手段と、前記鍵選択手段が選択した鍵を用いて暗号化コンテンツを復号する復号手段を備える。

さらに本発明では、暗号化コンテンツとメディアに固有なメディア鍵と鍵選択情報が記録された媒体を再生する端末であって、少なくとも前記暗号化コンテンツの復号鍵を含むライセンスを取得するライセンス取得手段と、前記ライセンスからコンテンツ鍵を取得するコンテンツ鍵取得手段と、前記暗号化コンテンツの復号に前記メディア鍵とコンテンツ鍵の何れを用いるかを前記鍵選択情報に基づいて判定する鍵選択手段と、前記鍵選択手段が選択した鍵を用いて暗号化コンテンツを復号する復号手段を備える。

さらに本発明では、暗号化コンテンツとメディアに固有なメディア鍵と鍵選択情報が記録された媒体を再生する端末であって、少なくとも前記暗号化コンテンツの復号鍵と利用条件を含むライセンスを取得するライセンス取得手段と、前記ライセンスからコンテンツ鍵を取得するコンテンツ鍵取得手段と、前記暗号化コンテンツの復号に前記メディア鍵とコンテンツ鍵の何れを用いるかを前記鍵選択情報に基づいて判定する鍵選択手段と、前記利用条件に基づいてライセンスに対応するコンテンツの利用可否を判定する利用可否判定手段と、前記鍵選択手段が前記メディア鍵を用いると判定するか、ライセンス鍵を用いると判定してかつ前記利用可否判定手段がコンテンツの利用が可能であると判定した場合に、前記鍵選択手段が選択した鍵を用いて暗号化コンテンツを復号する復号手段を備える。

さらに本発明では、暗号化コンテンツとメディアに固有なメディア鍵が記録された媒体を再生する方法であって、少なくとも前記暗号化コンテンツの復号鍵を含むライセンスを取得するライセンス取得処理と、前記ライセンスからコンテンツ鍵を取得するコンテンツ鍵取得処理と、前記暗号化コンテンツの復号に前記メディア鍵とコンテンツ鍵の何れを用いるかを判定する鍵選択処理と、前記鍵選択処理によって選択された鍵を用いて暗号化コンテンツを復号する復号処理からなる。

さらに本発明では、暗号化コンテンツとメディアに固有なメディア鍵と鍵選択情報が記録された媒体を再生する方法であって、少なくとも前記暗号化コンテンツの復号鍵を含むライセンスを取得するライセンス取得処理と、前記ライセンスからコンテンツ鍵を取得するコンテンツ鍵取得処理と、前記暗号化コンテンツの復号に前記メディア鍵とコンテンツ鍵の何れを用いるかを前記鍵選択情報に基づいて判定する鍵選択処理と、前記鍵選択手段が選択した鍵を用いて暗号化コンテンツを復号する復号処理からなる再生方法を提供する。

さらに本発明では、暗号化コンテンツとメディアに固有なメディア鍵と鍵選択情報が記録された媒体を再生する方法であって、少なくとも前記暗号化コンテンツの復号鍵と利用条件を含むライセンスを取得するライセンス取得処理と、前記ライセンスからコンテンツ鍵を取得するコンテンツ鍵取得処理と、前記暗号化コンテンツの復号に前記メディア鍵とコンテンツ鍵の何れを用いるかを前記鍵選択情報に基づいて判定する鍵選択処理と、前記利用条件に基づいてライセンスに対応するコンテンツの利用可否を判定する利用可否判定処理と、前記鍵選択処理が前記メディア鍵を用いると判定するか、ライセンス鍵を用いると判定してかつ前記利用可否判定手段がコンテンツの利用が可能であると判定した場合に、前記鍵選択処理が選択した鍵を用いて暗号化コンテンツを復号する復号処理を含む。

さらに本発明では、暗号化コンテンツを格納する媒体であって、メディアに固有なメディア鍵と、前記暗号化コンテンツが前記メディア鍵で暗号化されているか否かを示す鍵選択情報とが記録された媒体を提供する。

BRIEF DESCRIPTION OF THE DRAWINGS

図１は、本発明の一実施形態に係るコンテンツ再生システムの全体構成を示す図、
図２は、再生端末１０１の内部構成とメディア１０２に記録される情報を示す図、
図３は、ライセンスサーバ１０４の内部構成を示す図、
図４は、再生制御情報のデータ構造の一例を示す図、

図５は、ボタン表示用データのデータ構造の一例を示す図、
図６は、鍵制御情報のデータ構造の一例を示す図、
図７は、媒体固有情報のデータ構造の一例を示す図、
図８は、媒体鍵生成処理の処理手順を示すフローチャート、
図９は、再生制御処理の処理手順を示すフローチャート、
図１０は、コンテンツ再生処理の処理手順を示すフローチャート、
図１１は、コンテンツ鍵取得処理の処理手順を示すフローチャート、
図１２は、権利情報のデータ構造の一例を示す図、
図１３は、権利鍵取得処理の処理手順を示すフローチャート、
図１４は、コンテンツの再生可否判定処理の処理手順を示すフローチャート、
図１５は、権利判定処理の処理手順を示すフローチャートである。

DETAILED DESCRIPTION OF THE PREFFERED EMBODIMENTS

以下、本発明の実施の形態について、図面を参照しながら説明する。

（コンテンツ再生システムの全体構成）

図１は、本発明の一実施形態に係るコンテンツ再生システムの全体構成を示す図である。図１において、コンテンツ再生システムは、再生端末１０１と、メディア１０２と、表示装置１０３と、ライセンスサーバ１０４から構成される。メディア１０２は例えばＢＤディスクであり、表示端末１０３は例えばテレビモニターである。また、再生端末１０１とライセンスサーバ１０４は、インターネットなどのネットワーク１０５を介して接続される。

図２は、再生端末１０１の内部構成およびメディア１０２に記録される情報を示す図である。再生端末１０１は、読込手段２０１と、再生制御手段２０２と、復号手段２０３と、鍵制御手段２０４と、媒体鍵生成手段２０５と、操作手段２０６と、表示手段２０７と、権利処理手段２０８と、権利格納手段２０９と、権利取得手段２１０から構成される。再生端末１０１の一実装例としては、ＣＰＵ、ワークメモリ、フラッシュメモリ、ＢＤドライブ、リモートコントローラー、ビデオアダプター、ネットワークアダプターとから構成されるクライアントコンピュータシステムであり、読込手段２０１はＢＤドライブであり、操作手段２０６はリモートコントローラーであり、表示手段２０７はビデオアダプターであり、権利格納手段２０９はフラッシュメモリであり、権利取得手段２１０はネットワークアダプターであり、再生制御手段２０２と、復号手段２０３と、鍵制御手段２０４と、媒体鍵生成手段２０５と、権利処理手段２０８はＣＰＵとワークメモリを用いて動作するソフトウェアで構成する方法が挙げられるが、これに限定されるものではない。

図２に示すように、メディア１０２には再生制御情報２１１と、暗号化コンテンツ２１２と、鍵制御情報２１３と、媒体固有情報２１４が格納される。ＢＤメディアにはＵＤＦなどのファイルシステムを備えるため、図２で示した各情報はファイルシステム上の一つまたは複数のファイルとして記録される方法が一般的であるが、これに限るものではなく、例えば媒体固有情報はＢＤメディアのリードインエリアの特別な領域に記録する方法や、ＢＣＡ（Ｂｕｒｓｔ　Ｃｕｔｔｉｎｇ　Ａｒｅａ）を用いて記録する方法、さらには誤り検出符号に対して意図的に誤りを作成して情報を記録する方法などを用いても良い。

図３はライセンスサーバ１０４の内部構成を示す図である。ライセンスサーバ１０４は、権利送信手段３０１と、送信制御手段３０２と、権利生成手段３０３から構成される。ライセンスサーバ１０４の一実装例としては、ＣＰＵ、ワークメモリ、ＨＤＤ、ネットワークアダプターから構成されるサーバコンピュータシステムであり、権利送信手段３０１はネットワークアダプターであり、送信制御手段３０２と権利生成手段３０３はＣＰＵとワークメモリを用いて動作するソフトウェアで構成する方法が挙げられるが、これに限定されるものではない。

以上で、再生システムの全体構成に関する説明を終了する。次にメディア１０２に格納される情報のデータ構造に関して図４から図７を用いて説明する。

（再生制御情報のデータ構造）

図４は再生制御情報のデータ構造の一例を示す図である。再生制御情報は、以下の４つの情報から構成される

「再生番号」

再生制御情報に登録された項目を一意に特定するためのインデックス番号である。１から始まり、項目毎に１ずつ増加していく。

「再生コンテンツ」

各項目に対応するコンテンツを特定するための情報である。ＢＤメディアにはコンテンツが一つのファイルとして格納され、再生コンテンツには対応するコンテンツのファイル名が記録される。

「次再生番号」

当該コンテンツの再生が完了した場合に次に再生を行うべき項目の番号が記録される。例えば、１つめの項目では次再生番号が２となっているために、Ｏｐｅｎｉｎｇ．ｍｐｇの再生完了後には、Ｔｒａｉｌｅｒ．ｍｐｇの再生が始まる。

「不可時再生番号」

次再生番号で示されたコンテンツの再生が不可能であった場合に、代わりに再生すべき項目の番号が示される。例えば、２つめの項目では次再生番号が３に、不可次再生番号が４になっているために、Ｔｒａｉｌｅｒ．ｍｐｇの再生完了後に、Ｍｏｖｉｅ．ｍｐｇの再生が不可能な場合にはＷａｒｎｉｎｇ．ｍｐｇが再生される。なお、不可時再生番号が指定されていない場合には、次再生番号で示されるコンテンツの再生可否にかかわらず、次再生番号で示されるコンテンツの再生を強行することになる。

（暗号化コンテンツのデータ構造）

暗号化コンテンツは、ＭＰＥＧ２ビデオエレメンタリストリームとＭＰＥＧ２オーディオエレメンタリストリームをＭＰＥＧ２で規定された多重化方式によりトランスポートストリームとしたものを暗号化したデータである。暗号化にはＡＥＳ（Ａｄｖａｎｃｅｄ　Ｅｎｃｒｙｐｔｉｏｎ　Ｓｔａｎｄａｒｄ）を用い、アダプテーションフィールドを除くトランスポートストリームの各パケットのペイロードを暗号化する。

また、メニュー用のコンテンツの場合には、ビデオエレメンタリストリームとオーディオエレメンタリストリームに加えて、ボタン表示用のデータを格納することも可能である。ボタン表示用のデータはプライベートストリームとして記録されることが一般的であるが、これに限るものではない。図５はボタン表示用データのデータ構造の一例を示す図である。ボタン表示用データは、以下の６つの情報から構成される。

「ボタン番号」

ボタン表示用データに登録された項目を一意に特定するためのインデックス番号であり。１から始まり、項目毎に１ずつ増加していく。なお、当該メニュー用コンテンツの再生開始時には、１番目に登録されたボタンが選択状態になる。

「決定時再生番号」

当該項目のボタンに対してリモートコントローラーにて決定の指示がなされた場合に、再生を開始すべきコンテンツを特定するための番号である。ここで記述された番号は再生制御情報の再生番号に相当する。例えば、１つめの項目では、決定時再生番号として３が指定されているため、再生制御情報で再生番号として３が指定されているＭｏｖｉｅ．ｍｐｇが再生される。

「上移動」

当該項目のボタンを選択中にリモートコントローラーにて上移動の指示がなされた場合に、新たに選択状態となるボタンの番号を特定するための情報である。例えば、１つめの項目では４が指定されているため、４つめの項目で指定されるボタンが選択状態となる。

「下移動」

当該項目のボタンを選択中にリモートコントローラーにて下移動の指示がなされた場合に、新たに選択状態となるボタンの番号を特定するための情報である。

「左移動」

当該項目のボタンを選択中にリモートコントローラーにて左移動の指示がなされた場合

に、新たに選択状態となるボタンの番号を特定するための情報である。

「右移動」

当該項目のボタンを選択中にリモートコントローラーにて右移動の指示がなされた場合に、新たに選択状態となるボタンの番号を特定するための情報である。

（鍵制御情報のデータ構造）

図６は鍵制御情報のデータ構造の一例を示す図である。鍵制御情報は、以下の６つの情報から構成される

「再生コンテンツ」

各項目に対応するコンテンツを特定するための情報である。再生制御情報に記録される再生コンテンツと同様に、対応するコンテンツのファイル名が記録される。なお、再生制御情報とは異なり鍵制御情報では同一のコンテンツが複数回出現することはない。

「コンテンツ固有情報」

各コンテンツに対する鍵を生成するための、コンテンツ毎に定められた固有情報である。

「鍵生成情報」

各コンテンツに対する鍵を生成する際の、生成方法を指示するための情報である。媒体鍵、権利鍵、合成鍵の何れかが指定される。

「再生可否情報」

各コンテンツの再生可否を示す情報である。可能か不可能の何れかが指定される。なお、ここでは、可能か不可能かの何れかが指定されるとしたが、これだけに限るものではなく、例えば再生時の品質などを再生可否情報に含めても良い。

「コピー可否情報」

各コンテンツのコピー可否を示す情報である。Ｏｎｃｅ、Ｆｒｅｅ、Ｎｅｖｅｒの何れかが指定される。Ｏｎｃｅは１世代のみコピー可能、Ｆｒｅｅは自由にコピー可能、Ｎｅｖｅｒはコピー不可であることを示す。なお、ここでは、Ｏｎｃｅ、Ｆｒｅｅ、Ｎｅｖｅｒの何れかが指定されるとしたが、これだけに限るものではなく、例えばコピー時の品質やコピー先メディアを特定する情報などをコピー可否情報に含めても良い。

「対応権利方式情報」

鍵生成情報が権利鍵または合成鍵となっている項目に対して、対応する権利情報の方式を特定する情報である。例えば、３つ目の項目では、方式Ａが指定されているため、当該コンテンツに対する権利処理が許諾されるのは方式Ａで作成された権利のみである。

（媒体固有情報のデータ構造）

図７は媒体固有情報のデータ構造の一例を示す図である。媒体固有情報は、以下の２つの情報から構成される。

「機器固有情報」

再生機器に対して一意に付与されている機器固有情報である。

「暗号化媒体鍵」

媒体鍵を機器固有鍵によって暗号化したデータである。

本実施の形態では、媒体固有情報には機器毎に暗号化媒体鍵を記録する構成とした。ハックされるなどの理由で特定の再生機器が不正な機器となった際には、当該再生機器の機器固有情報および対応する暗号化媒体鍵を記録しないことによって、不正機器での再生を防止することが可能である。

なお、本実施の形態の方法では再生機器台数分だけ機器固有情報および暗号化媒体鍵を用意する必要がある。このような方法では、媒体固有情報のデータ量が不必要に大きくなるという問題があるために、二分木を用いた方法によってデータ量の圧縮を図っても良い。

以上で、メディア１０２に格納される情報のデータ構造に関する説明を終了する。以降では、再生端末１０１におけるメディア１０２の再生時の処理について図８から図１５を用いて説明する。

（媒体鍵生成処理）

再生端末１０１の電源投入直後やメディア１０２の挿入直後、ユーザによる再生開始指示時には、再生端末１０１は媒体鍵生成処理からメディア１０２の再生処理を開始する。

媒体鍵生成手段２０５では、媒体固有情報２１４から媒体鍵が生成される。図８は媒体鍵生成処理の処理手順を示すフローチャートである。

媒体鍵生成手段２０５は読込手段２０１を制御して、メディア１０２から媒体固有情報２１４を読み込む。媒体鍵生成手段２０５は機器毎に固有の機器固有情報を保持しており、読み込んだ媒体固有情報２１４から一致する機器固有情報を検索する。機器固有情報が一致する項目を発見した場合には、対応する暗号化媒体鍵を取得して、Ｓ８０３に遷移する（Ｓ８０１～Ｓ８０２）。

一致する機器固有情報が存在しない場合には、当該メディアの再生を停止して再生処理を終了する。例えば図７の例では機器固有情報０００３は媒体固有情報２１４には登録されていない。このために、機器固有情報０００３を持つ再生機器１０１では、メディアの再生を開始することなく停止することになる（Ｓ８０２～Ｓ８０４）。

次に、一致する項目が存在した場合の処理について説明する。媒体鍵生成手段２０５は機器毎に固有の機器固有鍵を保持しており、読み込んだ暗号化媒体鍵を機器固有鍵で復号する。復号して得られた値が媒体鍵となる（Ｓ８０３）。

得られた媒体鍵は鍵制御手段２０４に通知された後で、次に示す再生制御処理を開始する。

（再生制御処理）

媒体鍵生成処理によって媒体鍵を得た後で、再生端末１０１は再生制御情報２１１に従って、コンテンツの再生を開始する。

図９は再生制御手段２０２による再生制御処理の処理手順を示すフローチャートである。

再生制御手段２０２は読込手段２０１を制御して、メディア１０２から再生制御情報２１１を読み込む。最初に再生制御手段２０２は、再生制御情報２１１から再生番号１番を持つ項目を読み込む。ここで、指定された再生コンテンツの再生を復号手段２０３に指示する。なお、復号手段２０３でのコンテンツ再生処理については後述する（Ｓ９０１）。

再生番号１番で指定されたコンテンツの再生完了後は、次再生番号で指定される項目を再生制御情報２１１から読み込む。さらに指定された項目における再生コンテンツを取得する（Ｓ９０２）。

再生制御手段２０２は復号手段２０３と鍵制御手段２０４を経由して権利処理手段２０８に対して、Ｓ９０２で取得された再生コンテンツが再生可能か否かを問い合わせる。なお、復号手段２０３・鍵制御手段２０４および権利処理手段２０８での再生可否判定処理については後述する（Ｓ９０３）。

権利処理手段２０８に対する問い合わせの結果、再生可能であると判断された場合には、Ｓ９０２で取得された再生コンテンツを再生する。再生完了後はＳ９０２に遷移して順次コンテンツを再生していく（Ｓ９０４）。

一方、権利処理手段２０８に対する問い合わせの結果、再生不可と判断された場合には、不可時再生番号で指定される項目を再生制御情報２１１から読み込む。さらに指定された項目における再生コンテンツを再生する。再生完了後はＳ９０２に遷移して順次コンテンツを再生していく（Ｓ９０５～Ｓ９０６）。

（コンテンツ再生処理）

再生制御処理によって、特定コンテンツの再生開始が決定された場合には、再生端末１０１は、メディア１０２から暗号化コンテンツを読み込んで、コンテンツを再生する。

図１０は復号手段２０３および表示手段２０７によるコンテンツ再生処理の処理手順を示すフローチャートである。

復号手段２０３は鍵制御手段２０４を制御して、コンテンツ鍵を取得する。なお、鍵制御手段２０４でのコンテンツ鍵取得処理については後述する（Ｓ１００１）。

復号手段２０３は読込手段２０１を制御して、メディアから暗号化コンテンツを読み込む。この際に読み込む暗号化コンテンツは、既に述べた再生制御処理において、再生制御手段から指示されたファイル名で指定される暗号化コンテンツである。次に復号手段２０３は読み込まれた暗号化コンテンツがボタン用データを含むか否かを確認する。この確認は、例えば暗号化コンテンツに含まれる非暗号のＰＡＴ（Ｐｒｏｇｒａｍ　Ａｓｓｏｓｉ

ａｔｉｏｎ　Ｔａｂｌｅ）やＰＭＴ（Ｐｒｏｇｒａｍ　Ｍａｐ　Ｔａｂｌｅ）を確認し、プライベートストリームとして記録されているストリームが存在するかで判定することが可能であるが、これに限るものではない（Ｓ１００２）。

ボタン用データを含まない場合には、復号手段２０３は読み込んだ暗号化コンテンツをパケット単位で復号し、復号された平文コンテンツを表示手段２０７に対して送信する。表示手段２０７は平文コンテンツをデコードしてビデオデータの画面表示やオーディオデータの再生を行う（Ｓ１００３）。

ボタン用データを含む場合には、復号手段２０３はボタン用データを復号した上で、ボタン用データに含まれる決定時再生番号を取得する。復号手段２０３は再生制御手段２０２を制御して各決定時再生番号に対応する再生コンテンツのファイル名を取得する。このためには、再生制御手段２０２は読込手段２０１を制御して、メディア１０２から再生制御情報２１１を読み込み、指定された決定時再生番号に対応する再生コンテンツを取得する。取得された再生コンテンツのファイル名に対して、復号手段２０３は、鍵制御手段２０４を経由して権利処理手段２０８に対して、再生コンテンツが再生可能か否かを問い合わせる。なお、鍵制御手段２０４および権利処理手段２０８での再生可否判定処理については後述する（Ｓ１００４）。

こうして各ボタンに対応する再生コンテンツの再生可否を取得し終われば、復号手段２０３は読み込んだ暗号化コンテンツをパケット単位で復号し、復号された平文コンテンツを表示手段２０７に対して送信する。表示手段２０７は平文コンテンツをデコードしてビデオデータの画面表示やオーディオデータの再生を行う。

さらに、表示手段２０７はボタン用データに従い、ビデオデータにオーバーレイしてボタンを表示する。ここで、表示手段２０７はＳ１００４にて取得された、各ボタンに対応づけられた再生コンテンツの再生可否に応じてボタンの表示を変える。各ボタンに対応づけられた再生コンテンツが再生可能な場合には、当該ボタンは通常の表示を行うが、再生不可能な場合には当該ボタンはグレイアウトして表示する。さらに、当該ボタンを選択しての決定を不可とする（Ｓ１００３）。

（コンテンツ鍵取得処理）

コンテンツ再生処理の中で、コンテンツ鍵が必要となった際には、再生端末１０１はメディア１０２から鍵制御情報を読み込んで、当該コンテンツに対応するコンテンツ鍵を取得する。

図１１は鍵制御手段２０４および権利処理手段２０８におけるコンテンツ鍵取得処理の処理手順を示すフローチャートである。

鍵制御手段２０４は読込手段２０１を制御して鍵制御情報２１３を取得する。鍵制御手段２０４は、復号手段２０３から指定されたコンテンツに対応する項目を鍵制御情報２１３から取得する（Ｓ１１０１）。

次に鍵制御手段２０４はＳ１１０１で特定された項目から、鍵生成情報を取得する。鍵生成情報が媒体鍵である場合には、同じくＳ１１０１で特定された項目からコンテンツ固有情報を取得し、既に述べた媒体鍵取得処理にて取得された媒体鍵とコンテンツ固有情報から一方向関数を用いてコンテンツ鍵を生成する。なお、コンテンツ鍵の生成は一方向関数を用いる方法に限るものではなく、コンテンツ固有情報を媒体鍵で復号する方法や単純に両者を連結してハッシュを取るなど様々な方法がある。

また、鍵制御手段２０４はＳ１１０１で特定された項目から再生可否情報を取得する。再生可否情報が「不可」である場合には、コンテンツを再生しない。なお、本実施の形態では事前にコンテンツの再生可否判定を行って再生制御を行った上で、コンテンツの再生が指示されるため、この時点で利用不可となるのは不正攻撃などの異常が発生している場合のみである（Ｓ１１０２～Ｓ１１０３）。

鍵制御手段２０４が取得した鍵生成情報が媒体鍵では無かった場合には、鍵制御手段２０４は権利処理手段２０８を制御して、復号手段２０３から指定されたコンテンツに対応する権利鍵を取得する。なお、権利鍵取得処理については後述する（Ｓ１１０４）。

鍵制御手段２０４が取得した鍵生成情報が権利鍵であった場合には、Ｓ１１０４で取得

した権利鍵がそのままコンテンツ鍵となる。なお、鍵生成情報が権利鍵であった場合にも、権利鍵をそのままコンテンツ鍵とすることに限るものではなく、例えば権利鍵とコンテンツ固有情報から一方向関数を用いてコンテンツ鍵を生成するなどの方法も想定される。また、この際には、権利鍵からコンテンツ鍵の生成は鍵制御手段で行うだけではなく、権利処理手段で行うことも可能である。特に鍵制御手段と権利処理手段が異なる耐タンパモジュールとして実装されている場合には、権利鍵が鍵制御手段に出て行くことは無いため、セキュリティの観点で有効である（Ｓ１１０５）。

鍵制御手段２０４が取得した鍵生成情報が合成鍵であった場合には、Ｓ１１０４で取得した権利鍵と、既に述べた媒体鍵取得処理にて取得された媒体鍵から一方向関数を用いてコンテンツ鍵を生成する。なお、コンテンツ鍵の生成は一方向関数を用いる方法に限るものではなく、コンテンツ固有情報を媒体鍵で復号する方法や単純に両者を連結してハッシュを取るなど様々な方法がある。さらには、コンテンツ鍵の生成にコンテンツ固有情報も交えることも可能である。特に鍵制御手段と権利処理手段が異なる耐タンパモジュールとして実装されている場合には、鍵制御手段は媒体鍵とコンテンツ固有情報から情報を生成した上で、これを権利処理手段に通知し、権利処理手段は通知された情報と権利鍵からコンテンツ鍵を生成知ることにより、媒体鍵は権利処理手段に出て行くことはなく、権利鍵も鍵制御手段に出て行くことは無いため、セキュリティの観点で有効である（Ｓ１１０６）。

（権利鍵取得利処理）

コンテンツ鍵取得処理の中で、権利鍵が必要となった際には、再生端末１０１は権利格納手段２０９に格納された権利情報を読み込んで、当該コンテンツに対応する権利鍵を取得する。

図１２は権利情報のデータ構造の一例を示す図である。権利情報は以下の５つの情報から構成される。なお、権利情報の構成は以下の５つに限るものではなく特に再生回数や再生期限のように権利の条件に関する情報は様々な情報が想定される。

「権利方式情報」

権利情報の方式を特定する情報である。

「対応再生コンテンツ」

各項目で示される権利に対応するコンテンツを特定するための情報である。再生制御情報に記録される再生コンテンツと同様に、対応するコンテンツのファイル名が記録される。

「権利鍵」

各項目で示される権利に対応する権利鍵である。

「再生回数」

各項目で示される権利によって許可されたコンテンツの再生回数である。特に指定が無い場合には何回でも再生可能であることを意味する。

「再生期限」

各項目で示される権利によって許可されたコンテンツの再生期限である。特に指定が無い場合には、無期限に再生可能であることを意味する。

図１３は権利処理手段２０８および権利格納手段２０９における権利鍵取得処理の処理手順を示すフローチャートである。

権利処理手段２０８は権利格納手段２０９を制御して、権利情報を取得する。権利処理手段２０８は、鍵制御手段２０４から指定されたコンテンツに対応する項目を権利情報から取得する。なお、この際には鍵制御情報に含まれる対応権利方式情報で記載された方式が権利方式情報に指定されている項目のみが検索対象となる。例えば、鍵制御情報で対応権利方式情報が方式Ａとして指定されている場合には、コンテンツにＭａｋｉｎｇ．ｍｐｇが指定されていたとしても、図１３に示す権利情報であれば２行目の項目のみが検索対象となり、３行目の項目は検索対象とはならない（Ｓ１３０１）。

Ｓ１３０１にて指定されたコンテンツに対応する項目が存在しなかった場合には、指定されたコンテンツの利用は不可能であると判定され、権利鍵の取得は失敗する。なお、本実施の形態では事前にコンテンツの再生可否判定を行って再生制御を行った上で、コンテンツの再生が指示されるため、この時点で利用不可となるのは不正攻撃などの異常が発生

している場合のみである（Ｓ１３０２～Ｓ１３０３）。
Ｓ１３０１にて指定されたコンテンツに対応する項目が存在する場合には、さらに再生回数および再生期限に基づいてその利用可否を判定する。再生回数は０で無ければ、利用可能と判定する。再生期限は権利処理手段が備える時計との比較によって、指定された期限内であれば利用可能と判定する。再生回数と再生期限の双方で利用可能と判定されれば、結果としてコンテンツは利用可能と判定される。いずれか一方でも利用不可と判定されれば、コンテンツは利用不可と判定される（Ｓ１３０４）。
利用不可と判定された場合には、Ｓ１３０１にて指定されたコンテンツに対応する項目が存在しなかった場合と同様に、権利鍵の取得は失敗する（Ｓ１３０５～Ｓ１３０３）。
利用可能と判定された場合には、Ｓ１３０１にて指定されたコンテンツに対応する項目において権利鍵として指定されている情報を取得して成功となる（Ｓ１３０６）。
（再生可否判定処理）
再生制御処理の中で、コンテンツの再生可否判定が必要となった際には、再生端末１０１はメディアから鍵制御情報を読み込んで、当該コンテンツの再生可否を判定する。
図１４は鍵制御手段２０４および権利処理手段２０８におけるコンテンツの再生可否判定処理の処理手順を示すフローチャートである。
鍵制御手段２０４は読込手段２０１を制御して鍵制御情報２１３を取得する。鍵制御手段２０４は、復号手段２０３から指定されたコンテンツに対応する項目を鍵制御情報２１３から取得する（Ｓ１４０１）。
次に鍵制御手段２０４はＳ１４０１で特定された項目から、鍵生成情報を取得する。鍵生成情報が媒体鍵である場合には、同じくＳ１１０１で特定された項目から再生可否情報を取得し、設定された値が「可能」であれば指定されたコンテンツは再生可能と判定する。逆に設定された値が「不可」であれば、指定されたコンテンツは再生不可と判定する（Ｓ１４０２～Ｓ１４０３）。
鍵制御手段２０４が取得した鍵生成情報が媒体鍵では無かった場合にも、同じくＳ１１０１で特定された項目から再生可否情報を取得する。設定された値が「可能」であれば指定されたコンテンツは再生可能と判定する。なお、実際にはここで再生可能と判定されたとしても権利処理手段が権利鍵を取得しない限りはコンテンツ鍵を生成することができず、コンテンツを復号して再生することができないことには注意する必要がある。このために混乱を回避するためには、単に再生可否情報が「可能」であるからといって可能と判定するのではなく、権利鍵の有無を確認した上で再生可否を判定する方法が有効である（Ｓ１４０４）。
再生可否情報が「不可」であった場合には、権利処理手段にて、指定されたコンテンツの再生可否を判定する。なお、この権利判定処理については後述する（Ｓ１４０５）。
（権利判定処理）
再生可否判定処理の中で、権利判定処理が必要となった際には、再生端末１０１は権利格納手段２０９に格納された権利情報を読み込んで、当該コンテンツに対する再生可否を判定する。
図１５は権利処理手段２０８および権利格納手段２０９における権利判定処理の処理手順を示すフローチャートである。
権利処理手段２０８は権利格納手段２０９を制御して、権利情報を取得する。権利処理手段２０８は、鍵制御手段２０４から指定されたコンテンツに対応する項目を権利情報から取得する。なお、この際には鍵制御情報に含まれる対応権利方式情報で記載された方式が権利方式情報に指定されている項目のみが検索対象となる。例えば、鍵制御情報で対応権利方式情報が方式Ａとして指定されている場合には、コンテンツにＭａｋｉｎｇ．ｍｐｇが指定されていたとしても、図１３に示す権利情報であれば２行目の項目のみが検索対象となり、３行目の項目は検索対象とはならない（Ｓ１５０１）。
Ｓ１５０１にて指定されたコンテンツに対応する項目が存在しなかった場合には、指定されたコンテンツの利用は不可能であると判定する（Ｓ１５０２～Ｓ１５０３）。
Ｓ１５０１にて指定されたコンテンツに対応する項目が存在する場合には、さらに再生

回数および再生期限に基づいてその利用可否を判定する。再生回数は０で無ければ、利用可能と判定する。再生期限は権利処理手段が備える時計との比較によって、指定された期限内であれば利用可能と判定する。再生回数と再生期限の双方で利用可能と判定されれば、結果としてコンテンツは利用可能と判定される。いずれか一方でも利用不可と判定されれば、コンテンツは利用不可と判定される（Ｓ１５０４～Ｓ１５０６）。

（権利取得処理）

最後に権利取得手段２１０による権利取得処理について説明する。権利を取得する際には権利取得手段２１０は、ライセンスサーバ１０４の権利送信手段３０１とＳＡＣ（Ｓｅｃｕｒｅ　Ａｕｔｈｅｎｔｉｆｉｃａｔｉｏｎ　Ｃｈａｎｎｅｌ）を用いて暗号化通信路を確立する。その後、権利取得手段２１０は権利送信手段３０１に対して権利の送信を依頼する。なお、ライセンスサーバ内部での送信制御手段３０２および権利生成手段３０３を用いた権利生成や送信か非制御については本特許の内容とは関係ないため、説明を割愛する。

なお、本実施の形態ではライセンスに基づくコンテンツの利用可否による再生制御として、再生制御情報による再生経路の制御とボタン表示のグレイアウト有無という２つの例を示したが、これに限るものではない。例えば、ＤＶＤにおけるアングル切替に適用すれば、特定アングルだけが利用不可となるケースにて、当該アングルへの切替を禁止することも可能である。同様に音声・字幕ストリーム切替に適用すれば、特定音声・字幕ストリームが利用不可となるケースにて、当該音声・字幕ストリームへの切替を禁止することも可能である。

また、本実施の形態では鍵制御情報は暗号化されずに記録される構成となっているが、鍵制御情報中の再生可否情報やコピー可否情報の改竄による不正再生や不正コピーを想定すると、鍵制御情報は暗号化されるなどで保護されていることが望ましい。この場合には、媒体鍵で暗号化される方法が有効である。

なお、本実施の形態ではコンテンツの再生の場合に関して説明を行ったが、コンテンツのコピーに関しても同様の方法が適用可能である。

また、本実施の形態では利用不可となった場合には、その理由にかかわらず一律に同様の再生制御を行う例を提示したが、これに限るものではない。例えば、ライセンスが存在しない場合と、期限が切れていた場合で異なる再生制御を行っても良い。また、権利処理手段・権利格納手段・権利取得手段をカードなどのデバイスで実装し、再生端末から切り離すことができる場合には、そもそも権利処理手段への問い合わせが失敗する。このようなケースを想定して、権利処理手段が見つからなかった場合にも異なる再生制御を行っても良い。

なお、本実施の形態ではコンテンツ鍵取得処理および権利鍵取得処理では再生可否だけを扱う構成としたが、これに限るものではない。例えば、鍵制御情報および権利情報には再生可否に関する情報に加えて、ビデオストリームやオーディオストリームの再生品質に関する情報も記録することが可能である。このような場合には、コンテンツ鍵取得処理や権利鍵取得処理ではあわせて、これらの再生品質に関する情報も扱う。一般的には権利情報に記述される再生品質情報で鍵制御情報に含まれる再生品質情報を上書きすることが望ましい。このようにして取得された再生品質情報は、復号手段を経由して表示手段に通知され、表示手段では指定された品質でのみコンテンツを再生する。これによって、例えばＨＤ画質のコンテンツをＳＤ画質やＱＣＩＦ画質にダウンコンバートして再生するように強制的に指示することが可能となる。

また、本実施の形態では権利情報そのものに権利方式情報が記述されているとしたが、このままでは権利方式情報の改竄が行われる危険性がある。これは、各々の権利方式は別の事業者によって運営されるケースが一般的であり、悪意ある事業者が他の事業者に対して不正をはたらく危険性を排除できないためである。このような問題を回避するためには、権利情報には署名を付与し、この署名の付与者の証明書の中に方式情報を記載しておく方法がある。また、これ以外にも鍵制御手段と権利処理手段の間でＳＡＣ（Ｓｅｃｕｒｅ　Ａｕｔｈｅｎｔｉｆｉｃａｔｉｏｎ　Ｃｈａｎｎｅｌ）を用いて相互認証を行う場合には、

鍵制御手段は相互認証時に受信する証明書から相手側権利処理手段の方式を抽出して、対応権利方式情報に合致するかを確認するという方法もある。なお、相互認証を行う場合には媒体および権利格納手段にはＣＲＬ（Ｃｅｒｔｉｆｉｃａｔｉｏｎ　Ｒｅｖｏｃａｔｉｏｎ　Ｌｉｓｔ）が格納され、これによって不正なモジュールを排除する方法が一般的である。

なお、本実施の形態では鍵制御情報に「媒体鍵」が指定され、かつ再生可否情報に「不可」が指定されている場合には、無条件に再生不可となるが、これに限るものではない。このようなケースでも改めて権利処理手段に対して利用可否の問い合わせを行うことも想定される。

また、本実施の形態では鍵制御情報は暗号化コンテンツとは別にメディアに記録されるとしたが、これに限るものではない。例えば鍵制御情報を暗号化コンテンツに多重化することも可能である。この場合には、鍵制御情報とコンテンツの結びつきは明確になるため、鍵制御情報の中で再生コンテンツに関する情報は不要である。また、鍵選択情報が別のメディアに記録されることやネットワークを介して取得されるケースも想定される。特にコンテンツが一つのパッケージメディアだけに格納されるのではなく、別途ネットワークから追加コンテンツ取得してＨＤＤに記録するような場合には有効である。

なお、本実施の形態では権利情報には対応する再生コンテンツのファイル名が記録される構成としたがこれに限るものではない。例えば権利情報には各権利の識別子を記録し、鍵制御情報にも対応する識別子を格納することによって、この識別子で対応する権利を検索する方法も想定される。

また、本実施の形態では権利はライセンスサーバから取得するとしたがこれに限るものではない。例えば、メディアに権利が格納されており、ここから読みとる構成でも良い。

産業上の利用可能性

本発明にかかる暗号化コンテンツの再生装置および再生方法、ならびにそれに用いられるデータが格納された記録媒体は、従来型のコピー防止がなされたコンテンツとＤＲＭが適用されたコンテンツが混在するメディアでのコンテンツ再生に適しており、パッケージメディアやコンテンツ配信等の分野において有用である。

What is claimed is:

1、　暗号化コンテンツとメディアに固有なメディア鍵が記録された媒体を再生する再生端末であって、以下を含む：

・ ライセンス取得手段、
　少なくとも前記暗号化コンテンツの復号鍵を含むライセンスを取得する：

・ コンテンツ鍵取得手段：
　前記ライセンスからコンテンツ鍵を取得する；

・ 鍵選択手段、
　前記暗号化コンテンツの復号に前記メディア鍵とコンテンツ鍵の何れを用いるかを判定する；

・ 復号手段、
　前記鍵選択手段が選択した鍵を用いて暗号化コンテンツを復号する。

2、暗号化コンテンツとメディアに固有なメディア鍵と鍵選択情報が記録された媒体を再生する端末であって、以下を含む：

・ ライセンス取得手段、
　少なくとも前記暗号化コンテンツの復号鍵を含むライセンスを取得する；

・コンテンツ鍵取得手段、
　前記ライセンスからコンテンツ鍵を取得する；

・鍵選択手段、
　前記暗号化コンテンツの復号に前記メディア鍵とコンテンツ鍵の何れを用いるかを前記鍵選択情報に基づいて判定する；

・復号手段、
　前記鍵選択手段が選択した鍵を用いて暗号化コンテンツを復号する。

3、暗号化コンテンツとメディアに固有なメディア鍵と鍵選択情報が記録された媒体を再生する端末であって、以下を含む：

・ライセンス取得手段、
　少なくとも前記暗号化コンテンツの復号鍵と利用条件を含むライセンスを取得する；

・コンテンツ鍵取得手段、
　前記ライセンスからコンテンツ鍵を取得する；

・鍵選択手段、
　前記暗号化コンテンツの復号に前記メディア鍵とコンテンツ鍵の何れを用いるかを前記鍵選択情報に基づいて判定する；

・利用可否判定手段、
　前記利用条件に基づいてライセンスに対応するコンテンツの利用可否を判定する：

・復号手段、
　前記鍵選択手段が前記メディア鍵を用いると判定するか、ライセンス鍵を用いると判定してかつ前記利用可否判定手段がコンテンツの利用が可能であると判定した場合に、前記鍵選択手段が選択した鍵を用いて暗号化コンテンツを復号する。

4、クレーム1～3に記載の再生装置において、
　前記鍵選択情報にはコンテンツの識別子と、メディア鍵とコンテンツ鍵の何れを用いるかを示す鍵種別情報が格納される。

5、クレーム1～3に記載の再生装置において、
　鍵選択情報は暗号化コンテンツに多重化される。

６、クレーム１～３に記載の再生装置において、
鍵選択情報にはコンテンツに対応するライセンスの識別子が記載され、
前記コンテンツ鍵取得手段は前記ライセンス識別子で指定されるライセンスからコンテンツ鍵を取得する。

７、　暗号化コンテンツとメディアに固有なメディア鍵が記録された媒体を再生する方法であって、以下を含む；
・ ライセンス取得処理、
少なくとも前記暗号化コンテンツの復号鍵を含むライセンスを取得する；
・コンテンツ鍵取得処理、
前記ライセンスからコンテンツ鍵を取得する；
・鍵選択処理、
前記暗号化コンテンツの復号に前記メディア鍵とコンテンツ鍵の何れを用いるかを判定する；
・復号処理、
前記鍵選択処理によって選択された鍵を用いて暗号化コンテンツを復号する。
８、暗号化コンテンツとメディアに固有なメディア鍵と鍵選択情報が記録された媒体を再生する方法であって、以下を含む；
・ライセンス取得処理、
少なくとも前記暗号化コンテンツの復号鍵を含むライセンスを取得する；
・コンテンツ鍵取得処理、
前記ライセンスからコンテンツ鍵を取得する；
・鍵選択処理、
前記暗号化コンテンツの復号に前記メディア鍵とコンテンツ鍵の何れを用いるかを前記鍵選択情報に基づいて判定する；
・復号処理、
前記鍵選択処理が選択した鍵を用いて暗号化コンテンツを復号する。

９、暗号化コンテンツとメディアに固有なメディア鍵と鍵選択情報が記録された媒体を再生する方法であって、以下を含む；
・ライセンス取得処理、
少なくとも前記暗号化コンテンツの復号鍵と利用条件を含むライセンスを取得する；
・コンテンツ鍵取得処理、
前記ライセンスからコンテンツ鍵を取得する；
・鍵選択処理、
前記暗号化コンテンツの復号に前記メディア鍵とコンテンツ鍵の何れを用いるかを前記鍵選択情報に基づいて判定する；
・利用可否判定処理、
前記利用条件に基づいてライセンスに対応するコンテンツの利用可否を判定する；
・復号処理、
前記鍵選択処理が前記メディア鍵を用いると判定するか、ライセンス鍵を用いると判定してかつ前記利用可否判定処理がコンテンツの利用が可能であると判定した場合に、前記鍵選択処理が選択した鍵を用いて暗号化コンテンツを復号する。

１０、暗号化コンテンツを格納する媒体であって、以下のものが記録されている；
メディアに固有なメディア鍵と、
前記暗号化コンテンツが前記メディア鍵で暗号化されているか否かを示す鍵選択情報。

１１、クレーム１０の媒体において、

前記鍵選択情報にはコンテンツ識別子が記録される。

１２、クレーム１０の媒体において、
前記鍵選択情報にはライセンス識別子が記録される。

要約書
従来型のコピー防止がなされたコンテンツとＤＲＭが適用されたコンテンツが混在するメディアでのコンテンツ再生に適した暗号化コンテンツの再生装置および再生方法、ならびにそれに用いられるデータが格納された記録媒体を開示する。
メディアには各コンテンツが従来型のコピー防止がなされたコンテンツであるか、ＤＲＭが適用されたコンテンツであるかを示す情報を記録する。再生端末は、この情報に基づいてコンテンツの復号に用いる鍵を決定する。